System Wide Information Management

Program Overview and Security

Presented to: NATO/EUROCONTROL Air Traffic Management Security Coordination Group (NEASCOG)

SWIM Security Workshop

Presented by: Jim Robb

Date: 25 June 2010

Agenda

- **Program Overview**
- **Segment 1 Security**
- **Segment 2 Security**

Program Concept

SWIM is an IT infrastructure program that will operate in the background to provide data to authorized users

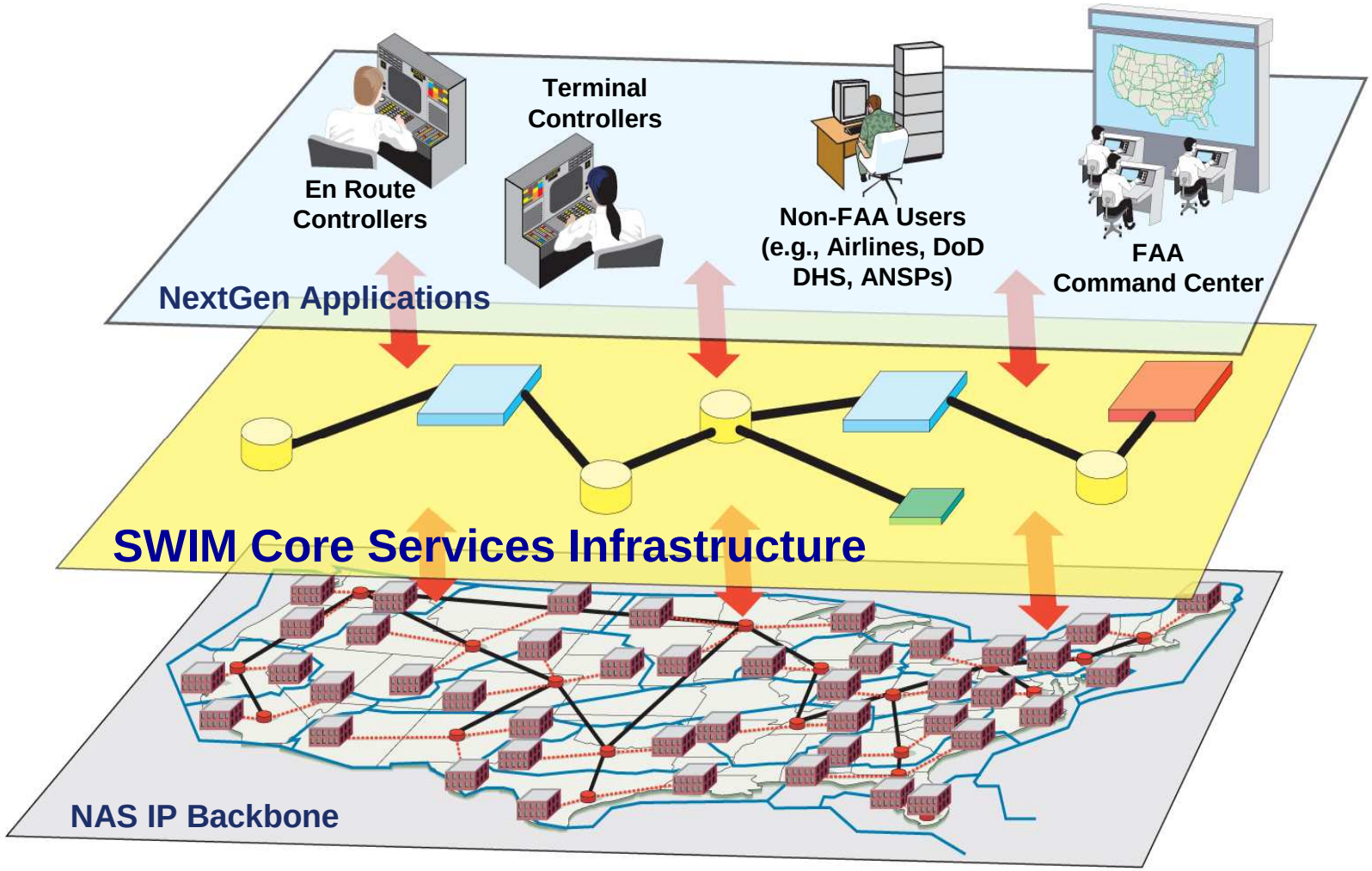
SWIM will:

- Implement a Service-Oriented Architecture (SOA) in the National Airspace System (NAS)
- Allow the FAA to create new system interfaces more quickly and more cheaply than is possible today
- Facilitate the increased data-sharing that is required for NextGen

SWIM is *not*:

- A set of avionics equipment
- A substitute for NAS modernization programs
- A telecom program

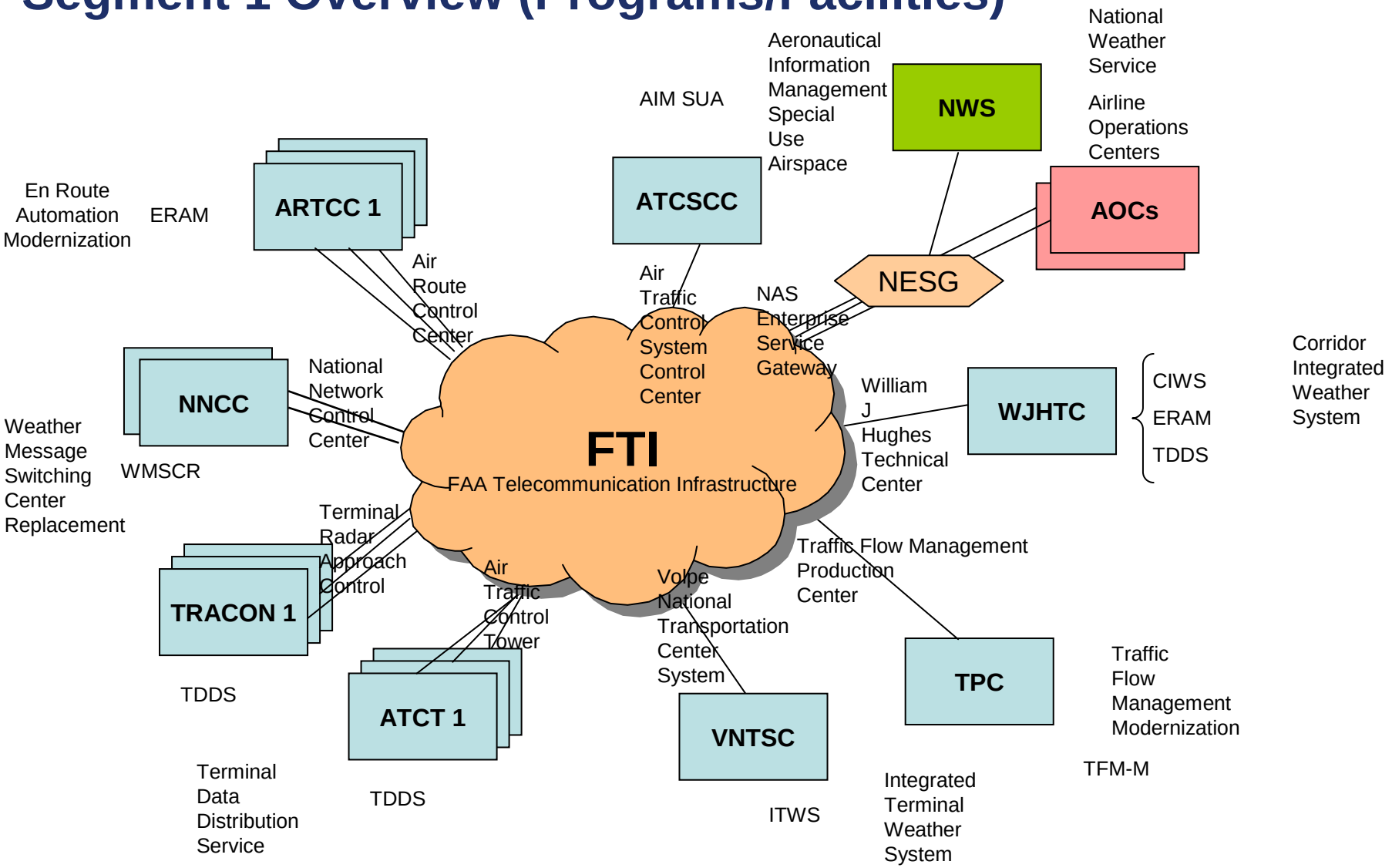
Conceptual Overview



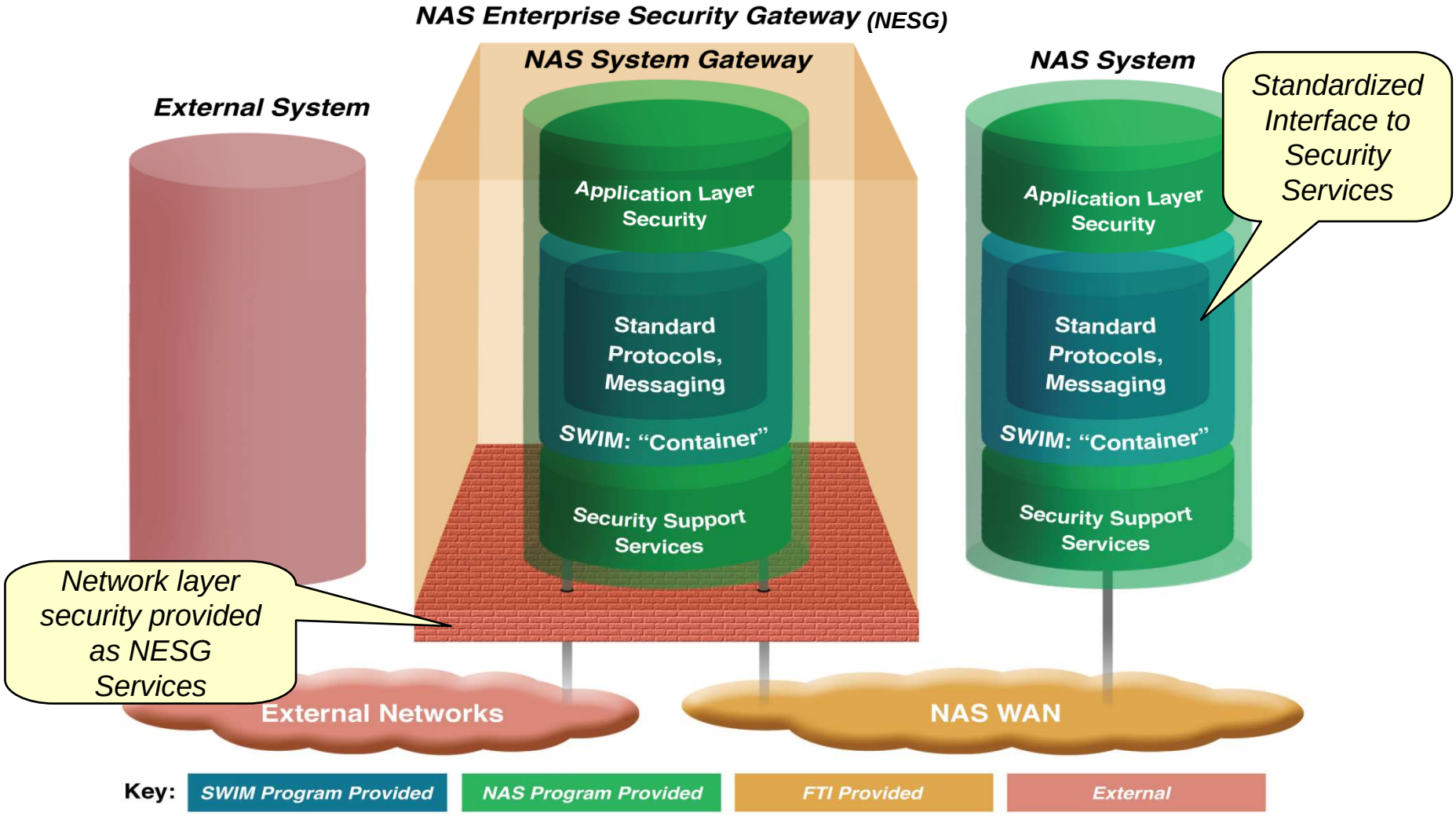
Agenda

- Program Overview
- **Segment 1 Security**
  - Architecture/Environment
  - SWIM Web Services Security Specification
- Segment 2 Security

Segment 1 Overview (Programs/Facilities)



SWIM Segment 1 Architecture – Security View



MITRE

SWIM Web Services (WS) Security Specification

- **SWIM policies require alignment with industry guidance for Web service security architecture and interoperability**
  - WS-I* Basic Security Profile
  - NIST** Guide to Secure Web Services
- **The industry guidance does not define any specific security architecture but describes a wide range of possible solutions**
- **The range of possible solutions is too broad to enable the ease of integration and service composition goals that are central to SWIM**
  - Proliferation of security controls could result in a web of point-to-point integrations
  - Differences in adopted security controls could undermine agility of SWIM SOA

*Web Services Interoperability Organization **National Institute of Standards and Technology_

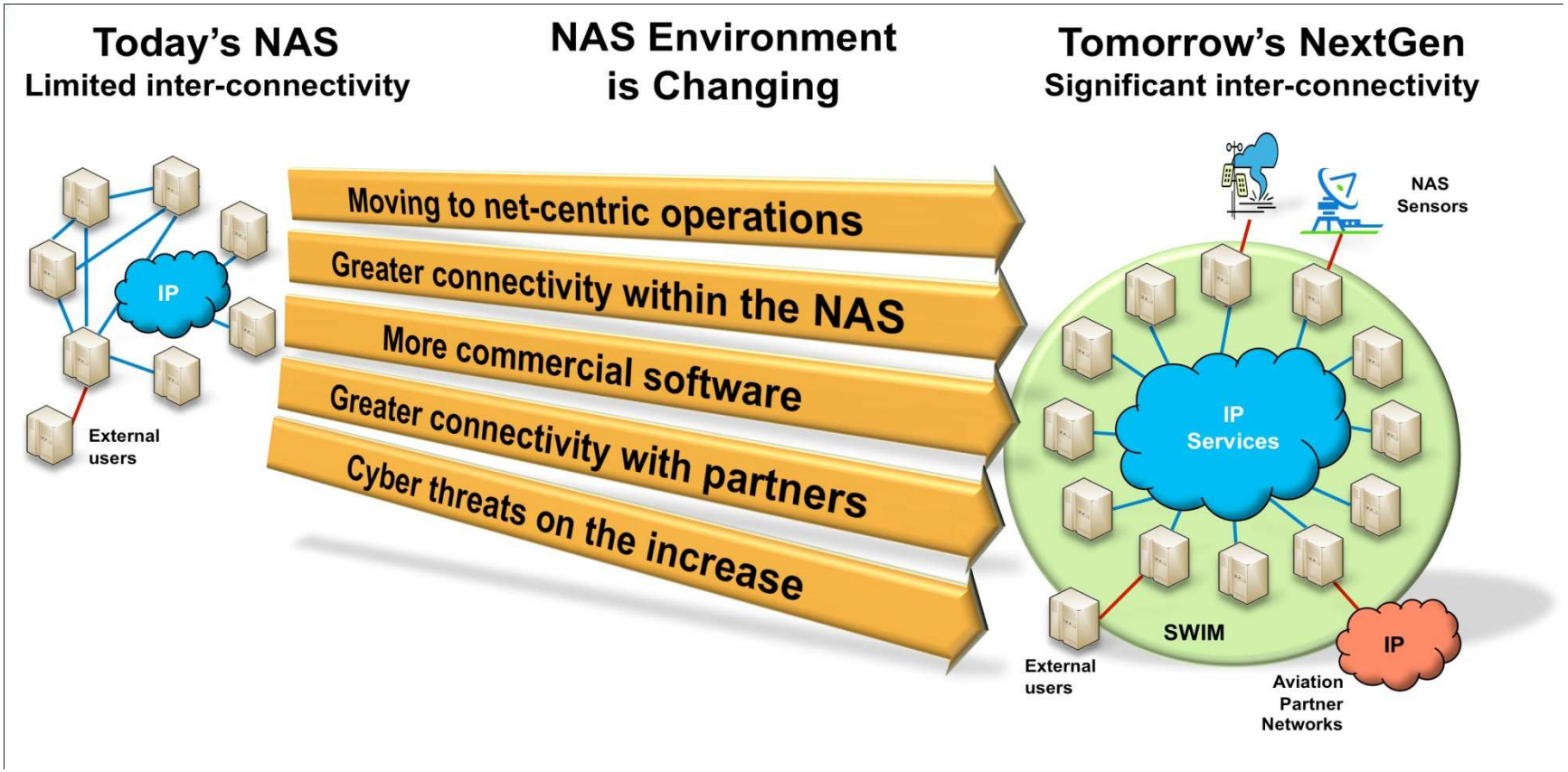
SWIM WS Security Specification Overview

- **Identifies the allowable security controls for Web Services in the SWIM environment**
- **Maps security controls to integration scenarios**
- **Defines specific requirements for security controls in token "profiles"**
  - Transport Layer Security (TLS) Profile
  - WS-Security Username Token Profile
  - WS-Security Binary Security Token Profile
  - Security Assertion Markup Language (SAML) Token Profile
- **Provides specific and verifiable requirements for each security control**
  - SOAP message security header content
  - Processing Rules
  - Allowable digest and encryption algorithms
- **The specification addresses only scenarios that involve message-level security for Simple Object Access Protocol (SOAP) messages**
  - No consideration for Representational State Transfer (REST)
    - content-based – Java Messaging System (JMS) destination security

Agenda

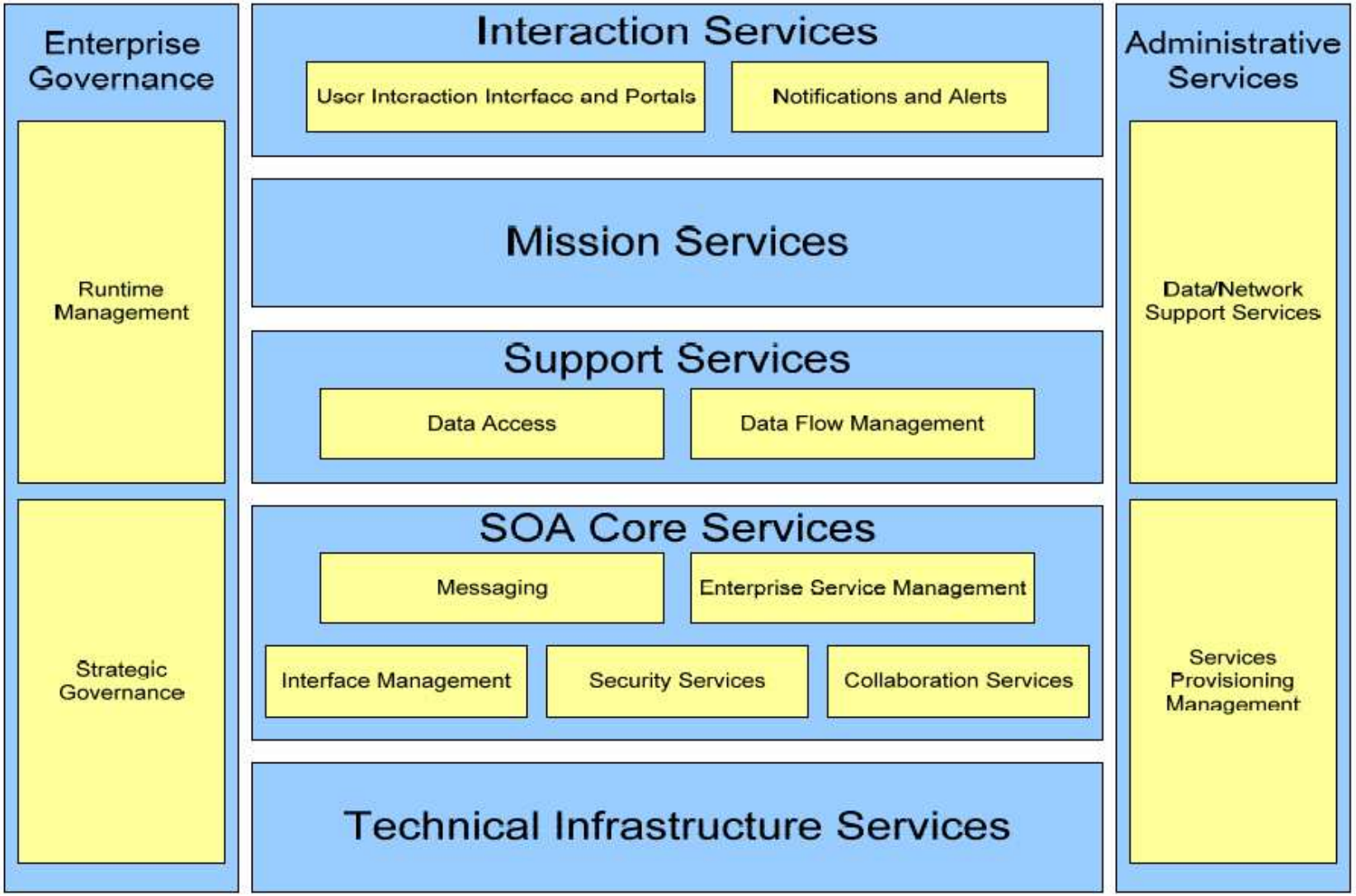
- Program Overview
- Segment 1 Security
- **Segment 2 Security**
  - Planning & Architecture
  - Prototyping

SWIM Segment 2
A CHANGING NAS ENVIRONMENT
REQUIRES AN ADDITIONAL CYBER SECURITY PERSPECTIVE

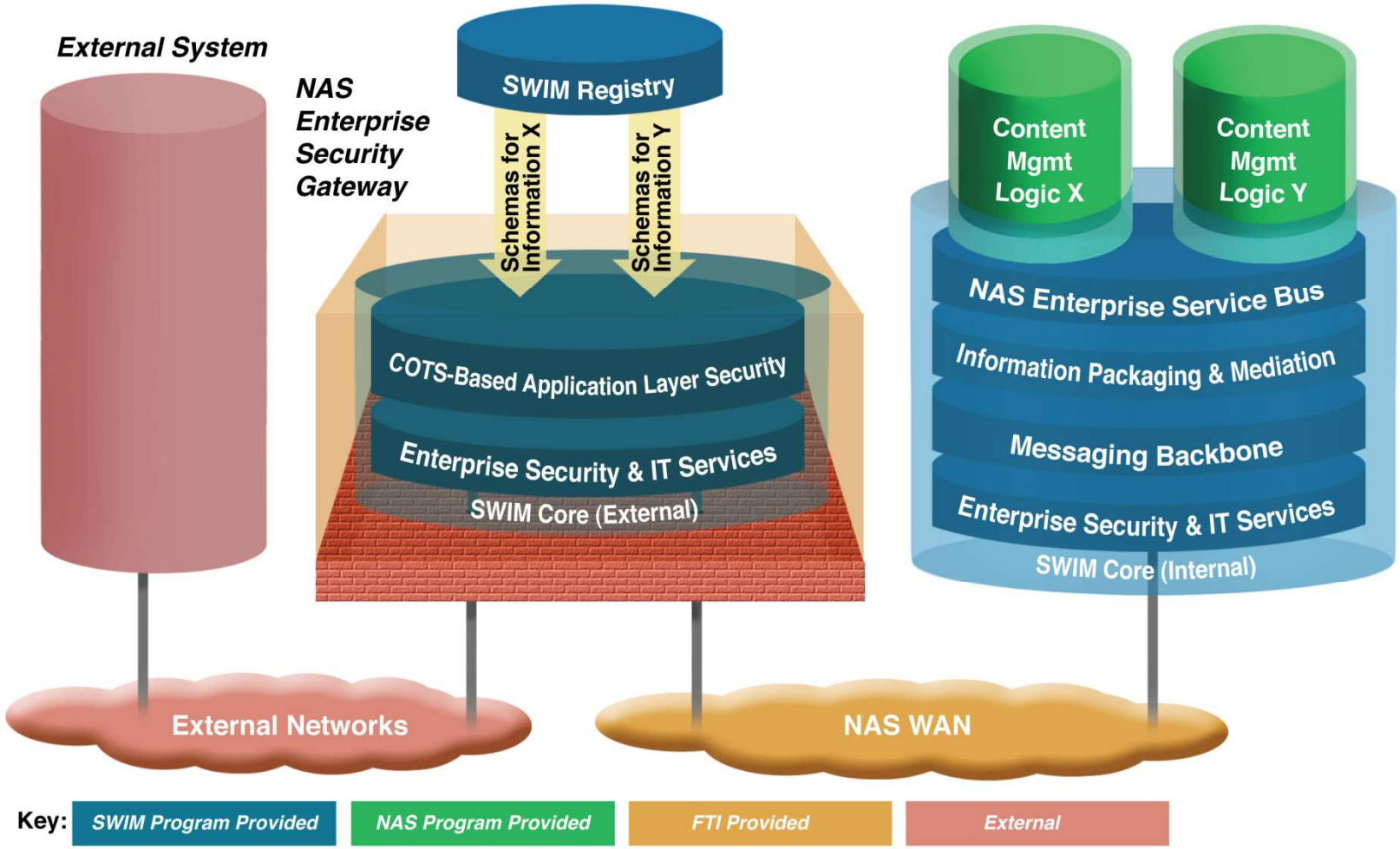


MITRE

Simplified NextGen NAS Services SV-4b

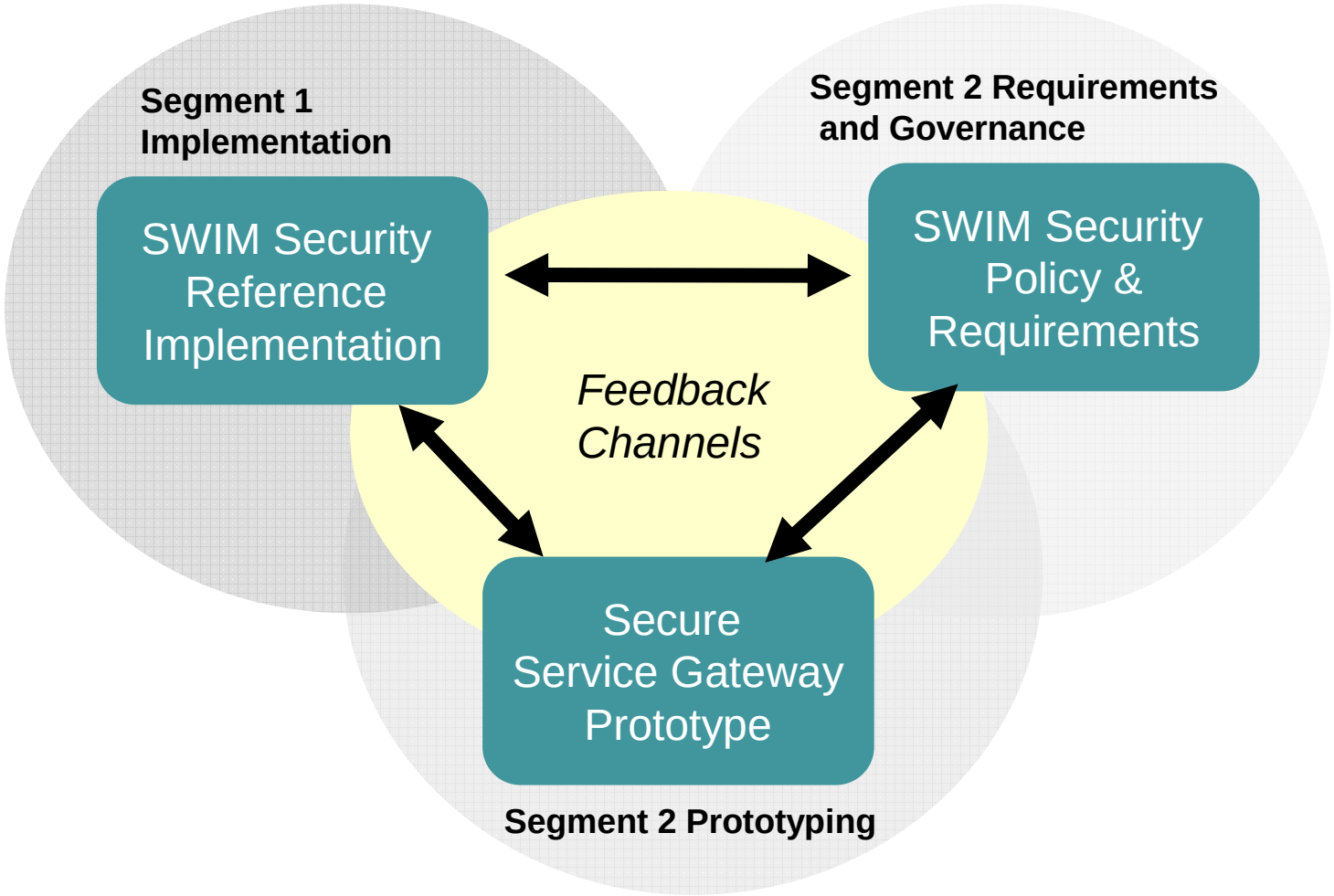


SWIM Segment 2 Core Architecture Security View



MITRE

SWIM Web Service Security Activity Landscape

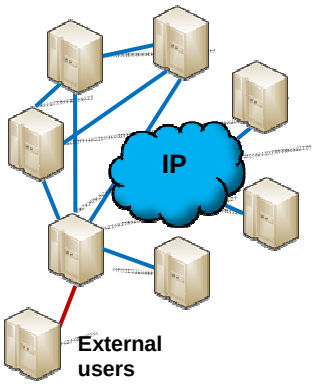


Options for Authentication subject identification when the integration involves an intermediary web service

- TLS with mutual Authentication?
  - NO. The subject is tied to the certificate used to establish the TLS connection
  - Subject would be the intermediate service instead of the initiator
- WS-Security Binary Security Token?
  - NO. The subject is tied to certificate used to sign the SOAP message
  - Subject would be the intermediate service instead of the initiator
- WS-Security Username Token?
  - Possible, but not practical
  - Username Token identifies the subject and is independent of the SOAP message; however, the password can be *in-the-clear* within the token or the ID store
- SAML Assertion?
  - YES! SAML Assertion provides subject information and is created independent of the SOAP message signature or transport
  - SAML Assertion is cryptographically signed by the issuer and provides additional security controls that can tie the assertion to the request message from the intermediary

SWIM Evolves to Meet NextGen Cyber Security Risks

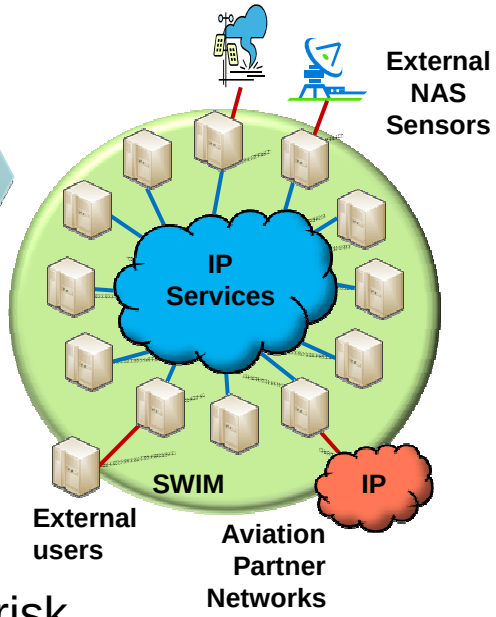
Today's NAS
Limited inter-connectivity



- **Planned NAS improvements**
  - **Moving to net-centric operations**
  - **Moving from custom to commercial software/standards**
- **Cyber threats on the increase**

Cyber risk

NextGen
Significant inter-connectivity



Greater use of Internet Protocol (IP) and greater connectivity require an effective Enterprise Information System Security Architecture

MITRE

SWIM Web Site

www.swim.gov